I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Living Our Lives Online: The Privacy Implications of Online Social Networking

DAVID HECTOR MONTES*

Abstract: Social networking web sites are more popular than ever. The population of users is increasing and diversifying, especially in terms of the age of users. The popular usage of these web sites greatly impacts user privacy. The privacy issues at stake include the interest in protecting children from exploitation and the increased use of social networking profiles by employers to screen job applicants. This note examines these concerns and their impact on the privacy of social networking web site users as well as potential legal mechanisms for addressing these issues.

I. INTRODUCTION

As technology advances, people find new ways to connect with others via the latest gadgets and software. In particular, many saw the increase in popularity of social networking sites, such as Myspace.com and Facebook.com, as an opportunity to expand our connections and make our world smaller.[1] These web sites now allow people to share

* David Montes is a J.D. candidate at The Ohio State University Moritz College of Law, expected to graduate in 2010. He graduated from Whittier College, in 2004, earning a B.A. *with distinction* in Biology and English. The author would like to thank his parents, Dave and Annabel for their unconditional love and support.

[1] Posting of Michael Arrington to TechCrunch, http://www.techcrunch.com/2009/01/22/facebook-now-nearly-twice-the-size-of-myspace-worldwide (Jan. 22, 2009); *see also* Posting of Michael Arrington to TechCrunch, http://www.techcrunch.com/2008/06/12/facebook-no-longer-the-second-largest-social-network (Jun. 12, 2008).

photos and messages with almost anyone they have ever met, and even many whom they have not.[2]

Much of our new networking occurs online and accessibility to every remark and picture posted online has increased. Living life online naturally results in decreased privacy. How do we accommodate an interest in guarding privacy if our culture encourages and facilitates documenting virtually every aspect of our online lives? Hollywood featured cybersecurity issues as early as 1995 in *The Net*, a film pitting Sandra Bullock against cyberterrorists who were able to manipulate her identity and records because she conducted most of her business and personal affairs via the Internet.[3] The film may have dealt with extremes during the Internet's early history. Still, it demonstrated our possible surrender of power if our dependence on technology becomes so great that it diminishes our real-world contact and forces us to rely on contact via the virtual world.

Although it may seem that, as the creators of our own online social networking profiles, we are able to construct our own online persona, this is not always the case. There is no law that prevents someone from establishing a fake account under another person's name, so long as the purpose for doing so is not to deceive others and gain some advantage. Moreover, fragments of information, either crafted under our authority or fabricated by others, are available by performing a Google search . . . forever. Thus, online social networking poses two threats: that information may be (1) available because of one's own role as the creator of the content, or (2) generated by a third party, whether or not it is accurate.

The increased use of social networking spans across generations, including minors and adults alike.[4] However, the privacy concerns associated with the two groups are different. Children's usage creates concerns of exploitation by sexual predators and harassment from

---

[2] *See* Facebook, http://www.facebook.com (last visited April 8, 2010); *see also* MySpace, http://www.myspace.com (last visited April 8, 2010).

[3] *The Net* (Columbia Pictures 1995).

[4] AMANDA LENHART & MARY MADDEN, PEW RESEARCH CTR., SOCIAL NETWORKING WEBSITES AND TEENS (2007), http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_SNS_Data_Memo_Jan_2007.pdf.pdf; AMANDA LENHART, PEW RESEARCH CTR., ADULTS AND SOCIAL NETWORK WEBSITES (2009), http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Adult_social_networking_data_memo_FINAL.pdf.pdf.

bullies. Adult users, on the other hand, may be subject to discrimination. Online social networking profiles are becoming a popular tool for employers in screening potential employees.[5] Additionally, law enforcement agencies have begun using social networking sites for investigative purposes. This note examines each of these threats to privacy posed by online social networking.

This note discusses online social networking behaviors, their impact on user privacy, and potential legal and legislative mechanisms for addressing these privacy concerns. Part II of this note examines the privacy implications of online social networking for children. In particular, it explores the legislation that first sought to protect children online and its evolution. Additionally, Part II reviews specific examples and statistics of children's activities online and the increasing documentation of our entire lives on the Internet. It includes a case study on the prosecution of Lori Drew, the Missouri mother who posed as a teenaged boy on the social networking site Myspace.com.[6] Finally, Part II examines the implications of children's activities and how new legislation is dealing with the issue, including legislation responding specifically to the *Drew* case. In Part III, this note examines how employers review social networking profiles as part of the employment screening process and explores how remedies to protect privacy may be implemented through technological safeguards.

Finally, Part IV of this note explores how law enforcement agencies are using online profiles for investigative purposes. Increasingly, law enforcement officers are screening social networking profiles to aid in criminal investigations. As a result, law enforcement agencies should be mindful of citizens' Fourth Amendment rights during these types of investigations.

II. PRIVACY PROTECTION CONCERNING CHILDREN

Many online privacy concerns involve personal data collection. Naturally, online privacy concerns surrounding the collection and dispersal of children's personal information are particularly important to both Congress and the public. In 1998, Congress passed the Children's Online Privacy Protection Act ("COPPA"), which sought to

---

[5] Posting of Jenna Wortham to Bits, http://bits.blogs.nytimes.com/2009/08/20/more-employers-use-social-networks-to-check-out-applicants (Aug. 20, 2009).

[6] U.S. v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

protect children's personal information from collection and dissemination on the Internet.[7]

In a report to Congress, the Federal Trade Commission ("FTC") explained that the foremost concern is the posting of children's personal information online.[8] The FTC was particularly concerned that such information could be found in public message-board forums and chat rooms that are accessible to all online users.[9] At the time, the Federal Bureau of Investigation and Justice Department feared that online media was quickly becoming the preferred resource for online predators to identify and contact children by using names and postal or email addresses.[10] Furthermore, the FTC felt that the web and its new tools for interaction were offering a message contrary to the traditional safety message routinely given by parents to their children: Don't talk to strangers.[11] At the time, the web was experiencing exponential growth. Its new forms of communication – message boards, instant messaging, e-mail, and chat rooms – did not inform children whether they were communicating with other children or adults during their online interactions. The FTC found this aspect of cyberspace to be particularly dangerous for children.[12] COPPA defines children as persons under the age of thirteen.[13] The FTC indicated that COPPA is intended to increase parental involvement in the online lives of their children in order to promote privacy and safety.[14]

In order to fully comply with COPPA's provisions, web site operators are required to provide notice to parents of the web site's

---

[7] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2000); *see also* Sarah Merritt, Comment: *Sex, Lies, and Myspace,* 18 ALB. L.J. SCI. & TECH. 593, 598 (2008).

[8] *See generally* FEDERAL TRADE COMMISSION, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (1998), *available at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf.

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *Id.*

[13] Children's Online Privacy Protection Act, 15 U.S.C. § 6501(1) (2000).

[14] *See* FEDERAL TRADE COMMISSION, YOU, YOUR PRIVACY POLICY AND COPPA: HOW TO COMPLY WITH THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT 1, *available at* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus51.pdf (last visited April 8, 2010).

information practices; obtain parental consent for the collection, use and/or disclosure of children's personal information; provide parents the opportunity to review collected information and an opportunity to refuse the operator's use or maintenance of the child's data; and establish and maintain reasonable methods to protect the confidentiality, security and integrity of the data collected.[15] The FTC issued a press release to web site operators informing them that compliance with new regulations was required to protect children's online privacy.[16]

In 2005, the FTC promulgated its proposed Children's Online Privacy Protection Rule,[17] which included a sliding scale that takes into account how obtained information will be used.[18] The Commission sought commentary on its proposed implementation of COPPA, and was prepared to "commence rulemaking proceedings, if warranted in response to the comments received."[19] The FTC eventually decided to promulgate its final rule without changes after the period of public comment.[20] Children's information that was to be distributed publicly required reliable forms of parental consent such as credit card verification, print and sign consent forms, or password and PIN protected email confirmations.[21]

In some cases, COPPA imposes fines for violations of the Children's Online Privacy Protection Rule. In 2006, Xanga.com, Inc. ("Xanga"), a website that hosts weblogs, photos and social networking profiles,[22] was a respondent in a complaint filed by the FTC for

---

[15] *See* 15 U.S.C. § 6502(b)(1) (2000); *see also* Merritt, *supra* note 7.

[16] Press Release, Federal Trade Commission, Web Sites Warned to Comply with Children's Online Privacy Law (Jul. 17, 2000), *available at* http://www.ftc.gov/opa/2000/07/coppacompli.shtm.

[17] *See* Press Release, Federal Trade Commission, FTC Seeks Comment on Children's Online Privacy Rule (Apr. 21, 2005), *available at* http://www.ftc.gov/opa/2005/04/coppacomments.htm [hereinafter FTC]; *see also* Press Release, Federal Trade Commission, FTC Retains Children's Online Privacy Protection (COPPA) Rule Without Changes (Mar. 8, 2006), http://www.ftc.gov/opa/2006/03/coppa_frn.shtm [hereinafter COPPA Without Changes].

[18] FTC, *supra* note 17.

[19] *Id.*

[20] COPPA Without Changes, *supra* note 17.

[21] FTC, *supra* note 17.

[22] Xanga.com, http://www.xanga.com (last visited April 8, 2010).

violating COPPA.[23] Xanga's violation resulted in a $1 million civil penalty and a consent decree to prevent them from committing future violations.[24] Despite Xanga's claims on its web site that children under age thirteen were not allowed to join, the FTC's complaint stated that Xanga knowingly collected information from underage children without parental consent.[25] COPPA's chief aim was to prevent the exploitation of children by protecting personal information, but as the popularity of the Internet grows, the exploitation of children is taking on a new form.

A. CHILDREN AND SOCIAL NETWORKING: NEW THREATS

New threats have emerged with the increased popularity of social networking web sites like Facebook and MySpace. While the law and its advocates continue to vigilantly protect children, sexual predators and cyberbullies continue to find ways to manipulate children online.[26] In early 2009, MySpace revealed that 90,000 registered sex offenders had been removed from its site after only two years.[27] MySpace uses software that cross-checks a database of personal information of registered sex offenders with users of the social networking site. Facebook uses a similar method for finding registered sex offenders on its site:

---

[23] *See* Press Release, Federal Trade Commission, Xanga.com to Pay $1 Million for Violating Children's Online Privacy Protection Rule (Sep. 7, 2006), *available at* http://www.ftc.gov/opa/2006/09/xanga.sthm.

[24] *Id.*

[25] *Id.*

[26] National Crime Prevention Council, Cyberbullying, http://www.ncpc.org/newsroom/current-campaigns/cyberbullying (last visited April 8, 2010); Cyber Bullying Statistics (Aug. 27, 2008), http://www.cyberbullyalert.com/blog/2008/08/cyber-bullying-statistics-that-may-shock-you; Chris Hansen, MSNBC, Dangers Children Face Online (Nov. 11, 2004), http://www.msnbc.msn.com/id/6083442; DAVID FINKELHOR, ET AL., CRIMES AGAINST CHILDREN RESEARCH CTR., ONLINE VICTIMIZATION: A REPORT ON THE NATION'S YOUTH (2000), *available at* http://www.missingkids.com/en_US/publications/NC62.pdf.

[27] Posting of Erick Schonfeld to TechCrunch, http://www.techcrunch.com/2009/02/03/thousands-of-myspace-sex-offender-refugees-found-on-facebook (Feb. 3, 2009).

> We have been working proactively with states' attorneys general to run their lists of registered sex offenders against our user base. Our team uses various internal tools to automatically find matches. Any potential matches are evaluated more fully by our internal team of investigation professionals.
>
> If we find that someone on a sex offender registry is a likely match to a user on Facebook, we notify law enforcement and disable the account. In some cases, law enforcement has asked us to leave the accounts active so that they may investigate the user further. [28]

In May of 2008, Facebook worked with forty-nine state attorneys general to identify and remove profiles of register sex offenders from their site.[29]

While there is a general awareness of and effort to protect children from online sexual predators, this seems to be less true about cyberbullies. The unique methods of cyberbullying and the undefined law identifying and protecting against it gives rise to the potential for exploitation of children and infringement of their privacy as they surf the web. The recent case of Lori Drew and her involvement in the suicide of Megan Meier illustrates the unique challenges of prosecuting and ultimately convicting those who use children's publicly posted personal information for exploitative purposes.

1. MEGAN MEIER: BACKGROUND

Like the majority of American teens,[30] Megan Meier, a thirteen-year old from Dardenne Prairie, Missouri, had an online profile on the social networking site Myspace.com.[31] Megan suffered from low self-esteem and depression.[32] Naturally, she was elated when she was

---

[28] *Id.*, quoting an official statement by Facebook's Chief Privacy Officer.

[29] Posting of Erick Schonfeld to TechCrunch, http://www.techcrunch.com/2008/05/08/breaking-facebook-to-announce-safety-and-privacy-deal-with-49-states (May 8, 2009).

[30] LENHART & MADDEN, *supra* note 4.

[31] *Case Not Closed in MySpace Suicide Hoax*, ABC NEWS, Nov. 30, 2007, http://media.abcnews.com/TheLaw/story?id=3936502&page=1.

[32] *Id.*

contacted, via Myspace, by sixteen-year-old Josh Evans, who claimed to live nearby.[33]

In the fall of 2006, Meier and Josh developed an online relationship that eventually ended in tragedy[34] Josh began to call Megan names, and left her this ominous final message: "The world would be a better place without you."[35] The message drove Megan to hang herself in her closet.[36]

Megan died without ever knowing the truth. Josh Evans was the creation of Lori Drew, the forty-seven year old mother of Megan's former friend.[37] Drew revealed to the police that she created the fake profile in order to gain Megan's trust and learn how Megan felt about her daughter.[38] A longtime family friend of Drew, Ashley Grills, admitted that she, along with Drew and Drew's daughter, set up the Josh Evans Myspace account.[39] However, Drew maintains that Grills was the "main instigator" in creating the Evans account and in beginning the online relationship with Megan.[40]

2. THE CASE

Missouri prosecutors were left with a difficult task in the aftermath of Megan's suicide. Once it was understood that Megan's suicide was linked to her online relationship with "Josh," prosecutors needed to determine if Drew's actions were criminal. A conservative perspective sees the incident as a case of conspiracy, or worse, blames

---

[33] *Id.*

[34] Christopher Maag, *A Hoax Turned Fatal Draws Anger But No Charges*, N.Y. TIMES, Nov. 28, 2007, at A28, *available at* http://www.nytimes.com/2007/11/28/us/28hoax.html?_r=1&pagewanted=print.

[35] *Id.*

[36] *Id.*

[37] Andrew Ramadge, Fake Profile Mum Could Be Charged, NEWS.COM.AU, Jan. 11, 2008, http://www.news.com.au/technology/fake-profile-mum-may-face-charges/story-e6frfrnr-1111115294742.

[38] *Id.*

[39] Jonann Brady, Exclusive: Teen Talks about her Role in Web Hoax That Led to Suicide, ABC NEWS, Apr. 1, 2008, http://abcnews.go.com/GMA/Story?id=4560582&page=1.

[40] *Id.*

Drew for Megan's death. A more liberal perspective concludes that as terrible as Drew's actions were, she was not in violation of the law. Notably, COPPA does not apply because this case does not involve the systematic collection of Megan's personal contact information. Drew was able to communicate with Megan because she had become her MySpace friend.[41] In this situation, the fact that the entire alleged crime occurred online poses its own set of challenges.[42] Missouri prosecutors were unable to bring charges against Drew based on her involvement in the case,[43] as they could not find any applicable state laws on which to ground their charges.[44]

Federal prosecutors in the Central District of California did find federal law applicable to the situation, and Drew was indicted by a grand jury in May of 2008.[45] Drew was charged with conspiracy under 18 U.S.C. § 371, accessing protected computers to obtain information under 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(B)(ii),[46] and aiding and abetting and causing an act to be done under 18 U.S.C. § 2(a).[47]

The indictment's most serious charge was the felony conspiracy. Under 18 U.S.C. § 371, if two or more people "conspire to commit any offense against the United States, or to defraud the United States," they can face a fine or up to five years in prison.[48] The prosecutors

---

[41] *Drew, supra* note 6, at 452.

[42] John S. Wilson, *MySpace, Your Space, or Our Space? New Frontiers in Electronic Discovery*, 86 OR. L. REV. 1201, 1202 (2007) ("In criminal cases, law-enforcement agencies and attorneys are turning in increasing numbers to social networking web sites such as MySpace and Facebook to gather evidence. Yet the legal profession's response to electronic evidence in both civil and criminal contexts can be described as advancing in fits and starts. The recent promulgation of new Federal Rules of Civil Procedure responded to the influx of burdensome electronic discovery requests by placing some limits on what types of electronic evidence are discoverable.").

[43] Linda Deutsch, *Prosecutors: Cyber Law Applies to Suicide Case*, USATODAY, Aug. 12, 2008, http://www.usatoday.com/news/nation/2008-08-12-327594069_x.htm.

[44] *Id.*

[45] U.S. v. Drew, 2008 WL 2078622 (C.D. Cal. 2008) (indictment) [hereinafter "Indictment"].

[46] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

[47] Indictment, *supra* note 45.

[48] 18 U.S.C. § 371 (2006).

sought to prove conspiracy by showing that Drew operated with another individual and violated the MySpace Terms of Use Agreement.[49] Under 18 U.S.C. § 1030(a)(2)(C), the U.S. Attorneys sought prosecution because of unauthorized access to protected computers, mainly the MySpace servers.[50] Additionally, they alleged that the offense was "committed in furtherance of . . . criminal or tortuous act[s] in violation of the Constitution or laws of the United States or of any State."[51] The indictment listed twelve overt acts of conspiracy which detailed Drew's actions from her first instance of obtaining a fake MySpace account on September 20, 2006 to October 16, 2006, when "Drew caused the Josh Evans MySpace Account to be deleted."[52]

3. CONVICTION AND DISMISSAL

After her trial, Drew escaped felony conviction, but was convicted of a misdemeanor based on her violation of the MySpace terms of service and "accessing MySpace servers to obtain information regarding" Meier.[53] Drew was found guilty of violating the Computer Fraud and Abuse Act[54] based on her unauthorized access of the MySpace computers and servers.[55]

U.S. District Judge George Wu eventually dismissed her conviction on July 2, 2009.[56] Judge Wu's acquittal of Drew stemmed

---

[49] Prosecutors found that Drew violated the following specifics of the MySpace Terms of Use Agreement; represented and warranted that all registration information submitted was truthful and accurate; solicited information from a person under age 18; and used the information obtained to torment and harass anther person. *See* Terms & Conditions, http://www.myspace.com/index.cfm?fuseaction=misc.terms (last visited April 8, 2010).

[50] 18 U.S.C. § 1030(a)(2)(C).

[51] 18 U.S.C. § 1030(c)(2)(B)(ii).

[52] Indictment, *supra* note 44, at 7-8.

[53] *Id.* at 9.

[54] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006).

[55] *Drew*, *supra* note 6, at 453.

[56] Linda Deutsch, Mother in Myspace Case Says It Was Properly Dismissed, COLUMBIA MISSOURIAN, Jul. 3, 2009, *available at* http://www.columbiamissourian.com/stories/2009/07/03/mom-myspace-case-says-it-was-properly-dismissed.

from his uneasiness about her conviction's sole basis being violations of the MySpace terms of service. Federal prosecutors had effectively manipulated a violation of MySpace terms of service so that it constituted the federal misdemeanor of unauthorized access of computers. Wu further supported his odd timing by referencing a case in which a judge changed his mind after ruling.[57] Drew's sentencing hearing was scheduled for May 2009, but Judge Wu postponed the hearing in order to thoughtfully consider Drew's motion to dismiss the case entirely.[58] As stated above, the jury convicted Drew in November of 2008 of three misdemeanor computer crimes, but the jury could not come to a decision on one felony count of conspiracy.[59] The felony charge carried a sentence of up to twenty years.[60] Judge Wu said that if Drew had been convicted by her peers on the felony count, he would have gone through with the sentencing.[61] Ron Meier, Megan's father, expressed his outrage outside of the Los Angeles court in May: "It just sickens me that it was an adult playing with the mind of a 13-year-old child."[62]

This case poses difficult issues. On one hand, Drew's actions and her role in Meier's death were reprehensible to a degree perhaps matched only by her apparent lack of remorse about the entire incident. Many would agree that Drew belongs in prison; the only question being whether three years would be a long enough sentence. But a prison sentence for Drew's behavior, while it would have deterred future cyberbullies, would have posed issues of its own. The case would have served as precedent for prosecuting anyone who is found to have violated a web site's terms of service. MySpace's terms state that misleading information is prohibited, so it might have followed that posting a less-than-current photograph of oneself

---

[57] *Id.*

[58] Posting of Alexandra Zavis to L.A. Now, http://latimesblogs.latimes.com/lanow/2009/07/myspace-sentencing.html (July 2, 2009).

[59] Scott Glover, *Jury Delivers Mixed Verdict in MySpace Bullying Trial*, L.A. TIMES, Nov. 27, 2008, at A1, *available at* http://articles.latimes.com/2008/nov/27/local/me-myspace-trial-verdict27.

[60] Zavis, *supra* note 58.

[61] Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRED, Jul. 2, 2009, http://www.wired.com/threatlevel/2009/07/drew_court.

[62] Zavis, *supra* note 58.

constitutes a violation. Such an interpretation would have been overbroad and vague. While it may have seemed just to put Drew in prison, her conviction would have harshly impacted future cases involving terms of service violations.

Drew's sentence would have been served for unauthorized use of a computer and for violating the terms of service for a popular online social networking site, but not for her role in Meier's death.[63] Her deletion of the fraudulent MySpace account shortly after Meier's suicide is telling, but to convict Drew under the prosecution's tenuous legal arguments would have negatively impacted the privacy that online social networking site users enjoy. Judge Wu stated that the prosecution under the Computer Fraud and Abuse Act ("CFAA"), via MySpace's terms of service, gave too much discretion to web site operators.[64] If the prosecution's legal argument was accepted, web site operators would decide what is criminal, and a breach of contract could be criminalized.[65] Wu articulated the inherent problem of allowing Drew's conviction to stand: "Is a misdemeanor committed by the conduct which is done every single day by millions and millions of people? . . . If these people do read [the terms of service] and still say they're 40 when they are 45, is that a misdemeanor?"[66] Undoubtedly, millions of social networking users quickly agree to terms without reading them at all, let alone reading them completely. Some of the appeal of many online services is the anonymity associated with their use. Arguably, online social networking sites are not completely anonymous because of their expression in the non-virtual world, but should someone be punished—prosecuted and potentially imprisoned—for creating an online alias so as not to draw attention to one's professional or public life? That Drew is free despite her essential role in pushing Meier to suicide may be unjust, but another injustice would have occurred if Drew's conviction had not been dismissed. To ensure that similar cases do not emerge, new legislation must provide for adequate remedies against cyberbullies while preserving privacy rights.

Legislation must be narrowly tailored to avoid being overbroad. Legislation should allow for the prosecution of specific unauthorized

---

[63] *Drew*, *supra* note 6, at 452-53.

[64] Zetter, *supra* note 61.

[65] *Id.*

[66] Zavis, *supra* note 58.

uses of computers and the Internet. This legislation must be crafted in a way so as not to criminalize trivial forms of misbehavior. One way to define the scope of such legislation would be to allow criminal prosecutions only in those cases where the victims would not be able to state a tort claim. Such a standard would not have allowed prosecution in the Drew case because Megan's parents had the right to pursue a civil wrongful death action. In this way, tort law principles could be applied to limit cyberbullying prosecutions to those situations where the actions of a cyberbully did not cause actual damages. On the other hand, there are arguments for criminalizing cyberbullying even when there is a civil remedy. These particular types of cases often present unique situations that are largely beyond the reach of traditional remedies. Although potential prison time seems unduly harsh, civil judgments may be inadequate.

From an advocacy standpoint, Drew's prosecution illustrates the dangers associated with the fraudulent use of online social networking sites – dangers that fall outside the traditional scope of societal fears of sexual predation and exploitation of minors. The potential for civil liability may not be enough of a deterrent to would-be cyberbullies. Drew's actions demonstrate that cyberbullies may be unconcerned with the consequences of their actions in the civil law system. If liability for civil damages is not enough to deter cyberbullying, then there is a need for increased deterrence through criminal prosecution.

B. LEGISLATIVE EFFORTS TO DATE

Legislation aimed at eliminating cyberharassment ranges from local city ordinances to state law to federal legislation.[67] The legislation has been met with varying degrees of support. While local ordinances have garnered support, proposed federal legislation has been challenged in Congress.[68]

After the national media attention given to Megan's suicide, Missouri aldermen in Dardenne Prairie worked to adopt a city

---

[67] David Ardia, *Missouri Town Makes Online Harassment a Crime After Megan Meier's Suicide*, CITIZEN MEDIA LAW PROJECT, Nov. 27, 2007, http://www.citmedialaw.org/blog/2007/missouri-town-makes-online-harassment-crime-after-megan-meiers-suicide; Wendy Davis, *Texas Lawmakers Crack Down on Fake Profiles*, MEDIAPOSTNEWS, Jun. 8, 2009, http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=107518; David Kravets, *Cyberbulling Bill Gets Chilly Reception*, WIRED, Sep. 30, 2009, http://www.wired.com/threatlevel/2009/09/cyberbullyingbill.

[68] Kravets, *supra* note 67.

ordinance that would outlaw harassment via electronic communication, including: Internet, email, and mobile phone text messaging.[69] The resolution states that "harassment and stalking by means of use of the Internet or other electronic communications"[70] is a growing problem. The resolution makes it illegal to engage in a pattern of conduct that would lead a reasonable person to suffer substantial emotional distress. The ordinance also states that it is illegal for an adult to contact a child under 18 years of age in a communication that would cause a reasonable parent to fear for their child's well-being.[71] Violation of the ordinance results in a misdemeanor charge if the violation is within the city limits, meaning a perpetrator has sent electronic messages to a victim within the city limits.[72]

The Texas state legislature called for even tougher standards than the Dardenne Prairie ordinance. It enacted legislation that made creating a web page on a social networking site in someone else's name without their permission a felony. Texas incorporated the law into the state's Penal Code.[73] The offense is punishable as a third-degree felony with a penalty of two to ten years in prison and up to a $10,000 fine.[74] For sending an email, instant message, text, or other electronic communication in another person's identity without permission and with the intent to harm or defraud someone, one can be charged with a misdemeanor and serve up to one year in jail and a maximum fine of $4,000.[75]

In April 2009, Representative Linda Sanchez (D-CA) introduced federal legislation entitled "Megan Meier Cyberbullying Prevention Act."[76] The proposed bill called for up to two years in prison for

---

[69] Ardia, *supra* note 67.

[70] Resolution No. 195, City of Dardenne Prairie, Missouri, Nov. 2007, *available at* http://www.slate.com/id/2178820/entry/2178821.

[71] *Id.*

[72] *Id.*

[73] TEX. PENAL CODE § 33.07 (2009), *available at* http://www.legis.state.tx.us/tlodocs/81R/billtext/pdf/HB02003E.pdf.

[74] *Id.*

[75] *Id.*

[76] Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. (2009), *available at* http://www.govtrack.us/congress/billtext.xpd?bill=h111-1966.

electronic speech meant to "coerce, intimidate, harass or cause substantial emotional distress to a person."[77] During a hearing of the Congressional Subcommittee on Crime, Terrorism and Homeland Security, Rep. Sanchez emphasized that the intrusive nature of cyberbullying warranted the proposal.[78] The chairman of the subcommittee, Rep. Bobby Scott (D-VA), cautioned legislatures "to be extremely careful before heading down [that] path."[79] His remark stemmed from a fear of the potential infringement upon free speech.[80]

The city ordinance from Dardenne Prairie seems to be the most effective approach as it serves to protect victims of cyberharassment without unduly impinging on the interests of the alleged perpetrators. Dardenne Prairie's ordinance specifically enumerates what type of harassment is punishable and what type of communication constitutes cyberharassment. The misdemeanor charge also seems consistent with the crime. While both the Texas and the proposed federal legislation do an adequate job of listing the types of actionable communication, they both also over-criminalize by making offenses felonies. Bullying is likely to be done by peers of schoolchildren and teens, and it seems unnecessarily harsh to convict another juvenile or peer (in the case of communication between those in their late teens) of a felony. A misdemeanor conviction demonstrates that cyberbullying is not acceptable and will not be tolerated. The fines and jail time associated with a misdemeanor crime seem adequate to curtail another case like that of Megan Meier.

III. USING SOCIAL NETWORKING SITES AS PART OF THE EMPLOYER SCREENING PROCESS

Employers have begun using the wealth of information available from online social networking profiles to screen potential employees. In the current economic climate, employers have smaller staffs to conduct interviews, so the cost-effective approach of using social networking sites to screen and recruit applicants has become

---

[77] *Id.*

[78] Kravets, *supra* note 67.

[79] *Id.*

[80] *Id.*

increasingly popular.[81] In order to view profiles of others on many social networking sites, one usually must be friends with that person, but this is not always the case. A Google search can often produce a link to Facebook.com which displays a user's profile picture, a sampling from their list of friends (including their profile pictures) and information about groups of which the user is a member.[82] According to a CareerBuilder.com survey, "twenty-two percent of employers" admit to using social networking sites to evaluate job candidates.[83] An additional nine percent intend to begin utilizing social networking sites in the same way.[84] The survey also illustrates that such screening methods have an effect on hiring decisions. Thirty four percent of hiring managers admit to having rejected an applicant based on information obtained from social networking sites, while only 24% said they were encouraged to hire job seekers based on online profiles.[85]

Anecdotal evidence can provide a quick lesson on the pitfalls of disclosing too much information online. The manager of a small consulting firm visited Duke University in 2006 to interview potential job applicants.[86] Before one interview, the manager decided to view an applicant's Facebook page.[87] On the page, "[s]he found explicit photographs and commentary about the student's sexual escapades,

---

[81] Candace Choi, *Be smart about what you post in online profile*, S.F. CHRON., Jan. 11, 2009, at C4, *available at* http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2009/01/10/BUCQ155BPC.DTL&type=tech.

[82] Pete Cashmore, *Facebook Profiles Will Appear in Google Results Next Month*, MASHABLE, Sep. 5, 2007, http://mashable.com/2007/09/05/facebook-search.

[83] Mike Hargis, *Social networking sites dos and don'ts*, CNN, Nov. 5, 2008, http://www.cnn.com/2008/LIVING/worklife/11/05/cb.social.networking/index.html?iref=newssearch.

[84] *Id.*

[85] *Id.*

[86] *See* Alan Finder, *For Some, Online Persona Undermines a Résumé*, N.Y. TIMES, Jun. 11, 2006, at A1, *available at* http://www.nytimes.com/2006/06/11/us/11recruit.html?_r=1&scp=1&sq=finder+online+persona&st=nyt (it is not known what level privacy settings this job applicant had on her online profile); *see also* Ian Byrnside, *Six Clicks of Separation: The Legal Ramification of Employers Using Social Networking Sites to Research Applicants*, 10 VAND. J. ENT. & TECH. L. 445, 447 (2008).

[87] Finder, *supra* note 86, at A1.

drinking and pot smoking."[88] The manager immediately decided the applicant would not receive a job offer.[89]

Career counselors and career web sites have recommended that job applicants censor their social networking profiles to present the most professional image of themselves during their job search. But should people be forced to alter their profiles?[90] Users can post an enormous amount of information in an online profile, from religious and political views to sexual orientation. Employers can potentially discriminate based on user profiles.

Fortunately, job seekers are protected from discrimination by federal and state laws that proscribe certain interview questions as off-limits. A series of federal laws forbid various types of employment discrimination. Title VII of the Civil Rights Act of 1964 prohibits employment discrimination based on race, color, religion, sex, or national origin.[91] The Age Discrimination in Employment Act of 1967 ("ADEA") protects individuals who are 40 years of age or older.[92] Titles I and V of the Americans with Disabilities Act of 1990 ("ADA") prohibit employment discrimination against qualified individuals with disabilities in the private sector, and in state and local governments.[93] Interviewers are prohibited from asking questions that would identify interviewees as members of any classes protected under these laws. A profile on Myspace or Facebook, however, could reveal the answer to an otherwise illegal question. An employer could ask appropriate and legal questions during an interview, but then discover the interviewee's religion or sexual orientation on his or her online profile and allow such information to influence the hiring decision.

There seems to be no adequate protection or remedy against such an injustice. Although such conjecture may seem paranoid, it is a real fear among modern job seekers. Alison Rosenblum, co-owner of a recruiting firm in upstate New York, says that when recruiters review

---

[88] *Id.*

[89] *Id.*

[90] *Cf.* Hargis, *supra* note 83.

[91] Civil Rights Act of 1964, Pub. L. No. 88-352, 78 Stat. 241, 255 (1964) (codified as amended at 42 U.S.C. § 2000e-2 (2009)).

[92] Age Discrimination in Employment Act of 1967, Pub. L. No. 90-202, 81 Stat. 602, 603 (1967) (codified as amended at 29 U.S.C. § 623 (2009)).

[93] Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 327, 370 (1990) (codified as amended at 42 U.S.C. § 12112 (2009)).

a profile, "there's a risk they'll judge you based on information that's not relevant to your job."[94] It may be prudent to maintain your online profile in the same fashion you maintain your résumé or curriculum vitae, but if an online profile is an outlet to share personal photos and opinions and connect with other people, it seems unfair that an employer may view it and judge based on professional standards.

The worry does not end with one's own photos and political views. Those whom one chooses to associate with on his or her network may hold, and more importantly display, controversial or polarizing views in politics or even an off-color sense of humor. David D. Perlmutter, director of the School of Journalism and Mass Communication and professor at the University of Iowa, noted the necessity of choosing friends wisely in the virtual world and the dangers of failing to do so.[95] Professor Perlmutter states, "friends can hurt your reputation as much as you can yourself: That embarrassing photo of you at a party, or that impolitic quote you made about your department, can be an unguided missile wandering about cyberspace ready to shoot down your good name."[96]

The viewers of an online profile also extend beyond a boss or potential boss. Could a potential client be upset by the fact that you are member of a liberal activist group? An employer's access to such information can stifle the political process. Employee fears that their political or social affiliations could adversely affect their work lives might stunt political activity. This situation could have far-reaching implications for democracy. One may argue that such information may be available via an organization's web site or other public information source, but the fact that social networking sites have become critical when reviewing a candidate or hiring a professional means that they may have an impact on hiring. The utility of social networking sites means that their use as a screening tool will likely remain. This is compounded by the fact that no law currently prevents employers from utilizing this particular screening technique. There is a litany of potential legal ramifications if the practice continues to be widespread: claims of invasion of privacy, defamation, violation of terms of service, and discrimination.[97]

---

[94] Choi, *supra* note 81.

[95] David D. Perlmutter, *Facebooking Your Way Out of Tenure*, THE CHRONICLE OF HIGHER EDUCATION, Jul. 3, 2009, http://chronicle.com/article/Facebooking-Your-Way-Out-of/46951.

[96] *Id.*

[97] Byrnside, *supra* note 86, at 459.

However, hiring managers have the law on their side because hiring decisions can be based on almost anything so long as overt discrimination cannot be proved.

Proving employer intent in employment discrimination cases is difficult. Creating effective legislation that protects the public against illegal discrimination will prove to be even more of a challenge. Potential legislation might expand upon existing employment discrimination laws and include clauses that specifically prohibit certain manners of obtaining information. In general, employment discrimination claims require the use of statistics to show disparate treatment in order to overcome that burden of proving intent.[98] Discrimination based on a candidate's online profile compounds the problem, resulting in so many variables that it becomes difficult to identify which factors the employer used to discriminate. Furthermore, restricting employers from accessing social networking sites would violate their First Amendment rights.

Increased legislation or legal remedies will not be effective in combating discrimination based on social networking profiles. If legislation is not the answer, perhaps there is a technological solution. Some proponents of using online social networking web sites feel that the user should bear the onus of maintaining the privacy of the user's own profile. Consistent with this view, Facebook has taken steps to increase the availability of privacy settings on its site.[99] New privacy settings are said to allow users greater control over what photos, updates, and personal details are viewed by friends and strangers on Facebook and the Internet at large.[100] Currently, the site has six privacy pages with a total of over thirty settings. Users must carefully navigate through each setting to limit or grant access to various aspects of their profiles.[101] The new settings are said to simplify the process: "[U]sers will be able to click on a lock icon to choose whether to show it to everyone, only their friends, friends of friends, members of professional or school networks or people on a customized list."[102]

---

[98] MICHAEL EVAN GOLD, AN INTRODUCTION TO THE LAW OF EMPLOYMENT DISCRIMINATION 11-12 (2001).

[99] Barbara Ortutay, *Facebook Plans to Simplify Privacy Settings*, ABC NEWS, Jul. 1, 2009, http://abcnews.go.com/Technology/wireStory?id=7979499.

[100] *Id.*

[101] *Id.*

[102] *Id.*

It is unknown whether other similar social networking sites will emulate Facebook's efforts, but given Facebook's popularity, it seems likely that competitors will follow suit. This technological solution will be more effective in minimizing the chance that an employer will discriminate—consciously or not—based on a social networking profile. In the context of hiring, technological remedies rather than legal action or legislation seem to be the best solution to the potential pitfalls of online social networking.

Individual profile users need continued education about the need for professionalism when using online social networking media. Employers should also be educated on the subject of social networking sites. Reviewing social networking sites could help an employer attempt to more fully understand job applicants and gain insight into their personalities. However, human resource departments should be warned that it may not be wise to invest too much energy in reviewing online profiles, particularly because they do not tell the whole story and because unconscious bias may affect hiring decisions. Similar to the way in which diversity and cultural sensitivity training have become routine in the workforce, so too should employers be educated about how social networking sites are utilized and users' expectations of privacy. Hiring officials should be made aware that if they choose to continue to review social networking sites, they may become privy to information they would not otherwise know and should not let such information negatively impact their decisions. In addition, employers should be made aware that a cursory view of a Facebook profile may lead to misunderstanding an applicant. Therefore, online profiles, on their face, should not be the deciding factor in hiring decision. It is likely that as a generation of MySpace and Facebook users mature into positions of power and become decision makers in hiring, they may redefine expectations of the separation between public and private lives.

IV. LAW ENFORCEMENT INVESTIGATIONS: THE BENEFITS OF REVIEWING SOCIAL NETWORKING PROFILES

Employers are not the only ones utilizing social networking sites as a way to learn more about someone. Law enforcement agencies have recently taken their investigation and crime prevention efforts online. A 16-year-old boy was arrested in Denver, Colorado after law enforcement personnel found photographs of him posing with

firearms on his MySpace profile.[103] A group of concerned parents became aware of the photographs and promptly alerted authorities.[104] The youth was arrested at his home and charged with three counts of juvenile possession of a handgun.[105]

There have also been instances when law enforcement was too late for prevention, but social networking sites proved useful in gathering evidence of crimes. MySpace assists police officers with 150 investigations per month and the company has a twenty-member law enforcement team that handles 350 phone calls per month from nearly 800 agencies.[106] In Tacoma, Washington, officers used MySpace to prove motive in a triple homicide.[107] Officers were able to confirm that the victims and suspects knew each other by examining the parties' "friends lists."[108] In Boulder, Colorado a detective assembled a lineup of potential suspects in a sexual assault case from portraits displayed on MySpace profiles.[109]

The use of online social networking web sites as a tool for law enforcement investigations complicates the discussion about using the sites for less serious endeavors such as employment screening. Online profiles cannot be written off as mere entertainment or as simply the modern method to communicate, when they have proven useful in finding otherwise unattainable evidence of criminal behavior. Perhaps guidelines or regulations could provide a useful barometer for how online networking profiles should be used and also outline the limitations and dangers of allowing seemingly private personal information to color one's judgment in areas such as hiring.

In searching for these guidelines, perhaps we should find direction from the Fourth Amendment. The investigations being conducted by law enforcement agencies are governed by search and seizure

---

[103] The Associated Press, *Teen arrested for blog gun photos*, MSNBC.COM, Feb. 23, 2006, http://www.msnbc.msn.com/id/11514585.

[104] *Id.*

[105] *Id.*

[106] Andrew Romano, *Walking a New Beat: Surfing MySpace.com helps cops crack the case*, NEWSWEEK, Apr. 24, 2006, at 48, *available at* http://www.newsweek.com/id/47100.

[107] Paul Sand, *MySpace: Meet people, talk music, fight crime,* NEWS TRIB. (Tacoma, Wash.), Mar. 12, 2006, at A1.

[108] *Id.*

[109] Romano, *supra* note 106.

doctrine. But unlike the tangible places of interest that are normally part of the discourse of Fourth Amendment searches, Facebook and MySpace profiles exist as intangible places.[110] What needs to be determined is when law enforcement agencies need a warrant to investigate an online profile and when such information is considered to be in plain view.[111] Under the plain view doctrine, law enforcement can search in an open field even if it is privately owned,[112] they can go further and search a barn that is located in an open field,[113] or they may view items inside of a house if their entry into the abode was lawful.[114]

Some have suggested that profiles on Facebook or MySpace are akin to public storage facilities.[115] Under this theory, an online profile would be analyzed in the same fashion as a "closed container."[116] However, what this analogy fails to consider is that even if an online profile is set to private, one's online friends have access to view the contents of the profile.[117] Thus, law enforcement officers could, with a friend's permission, use the friend's profile to gain access to the profile of the person being investigated. This invasive situation would allow police to bypass the warrant system. In this case, a warrant should be required because it is not reasonable for someone to expect that his or her online friends would work with a law enforcement agency to gain access to his or her profile.

---

[110] *See generally* Matthew J. Hodge, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and Myspace.com*, 31 S. ILL. U. L.J 95 (2006).

[111] "[O]bjects, activities, or statements that [one] exposes to the 'plain view' of outsides are not 'protected' because no intention to keep them to [oneself] has been exhibited." Katz v. U.S., 389 U.S. 347, 361 (Harlan, J., concurring).

[112] Oliver v. United States, 466 U.S. 170, 181 (1984).

[113] United States v. Dunn, 480 U.S. 294, 304-5 (1987).

[114] Ker v. California, 374 U.S. 23, 43 (1963).

[115] Hodge, *supra* note 110, at 119.

[116] *Id.*

[117] http://www.facebook.com/privacy/explanation.php. This is largely dependent upon one's privacy settings, specifically if this information is available to Friends or Friends of Friends. *Id.*

V. CONCLUSION

We must not be too quick to condemn online social networking as a facilitator of harassment or as an advanced technological evil that poses grave danger to our children. Like all advanced tools, online social networking is not inherently dangerous, even with the risks it can pose to its youngest users. Allowing our fears and emotions to get the better of us can have serious legal implications. Perhaps the decision to prosecute Lori Drew was based too much upon the emotions surrounding the tragedy of a young Midwestern teen being driven to suicide.

In post-9/11 America, we have been too eager to sacrifice our own liberties and privacy in favor of increased protection. This protection has proven too costly. New technologies could have quickly discovered the authenticity of a certain Myspace account used to torment Megan Meier, but sacrificing the anonymity offered from some social networking sites could be an even greater risk to the new communities that have been created via online social networking. For example, President Obama's success in the 2008 presidential election owes much of its success in grass roots campaigns to utilizing social networking sites such as Facebook.[118]

Lawmakers and policy analysts need to be aware of the rapidly changing dynamics of the cyberworld. Impulsively enacting legislation whenever tragedy strikes may lead to legislation that we regret. Society must understand that new technologies and the ways we use them will always pose a risk, particularly if we continue to insist on living our lives online. We must strike a careful balance between our need to feel safe online and to ensure our children are safe, and our desire to participate in a culture of disclosure on the Internet. But even beyond that, our entire notion of privacy must evolve with our ever-increasing use of online social networking. In a sense, we are all becoming public figures as we use our Myspace, Facebook, Twitter, Flickr, and other social networking accounts, but the old adage that public figures surrender their privacy is not consistent with the new online culture we have embraced. Ultimately, legislation must keep pace with our changing online culture, and litigation should be employed for the cases that are too close to call. There needs to be a balance between privacy rights and the evolved

---

[118] Ellen McGirt, *How Chris Hughes Helped Launch Facebook and the Barack Obama Campaign*, FASTCOMPANY.COM, Mar. 17, 2009, http://www.fastcompany.com/magazine/134/boy-wonder.html.

concept of privacy under which the law will protect us from unwanted intrusion.

Some may argue that in this new era of online social networking, we must be vigilant and conscious of how we are creating our online personas. But is the same true for children? Setting age restrictions for use of certain web sites may help, but recent studies indicating a biological basis for teens' failure to understand the full ramification for their actions call into question the efficacy of these protections.[119] Children and teens can easily disregard web site age restrictions, and relaxed attitudes can contribute to minors' inability to understand that the restrictions are in place specifically to keep them from the hazards of online social networking. Is the law enough to protect our children from the potential dangers of socializing online? These questions remain unanswered for now. Hopefully the tragedy of Meier's death has made it apparent that the current law does not protect children in the area of child exploitation. But we must also remember that we cannot rely too heavily on the law to completely shield us from the malevolence of others.

Some legislation introduced in the wake of Meier's death seems promising and could be effective in protecting privacy interests in a variety of contexts. The Texas legislature's statute, although too harsh in penalty, provides a good model of how to protect against those who create fake profiles to sabotage a colleague's promotion or to fabricate evidence in a criminal investigation.

Additionally, in the context of the hiring process, technological solutions are the best way to minimize the effect of discrimination based on an online profile. People need to have expanded options to decide which aspects of a social networking profile third parties will be able to access.

Despite the apparent risks involved in social networking, the wealth of information available online can facilitate law enforcement investigations. This use of technology should be encouraged, as it increases the efficiency of law enforcement investigations. But even this socially beneficial use of online information must occur within constitutional boundaries.

The solution to protecting privacy in the realm of social networking does not lie in one legislative solution or solely in the best technological upgrades. Instead, it lies in a combination of the two as well as in our own personal responsibility. Regardless of what legislative and technological protections emerge, we all must be

---

[119] *See generally* Claudia Wallis, *What Makes Teens Tick*, TIME, Sep. 26, 2008, http://www.time.com/time/magazine/article/0,9171,994126,99.html.

cautious about the information we disclose online and to whom we disclose that information.